CROCKER & CROCKER, P.C.

ATTORNEYS AT LAW

PATRICK D. CROCKER
patrick@crockerlawfirm.com

February 23, 2009

Ms. Marlene H. Dortch
Office of the Secretary   *Filed Electronically Via ECFS*
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

       RE: Conexiz Corporation
                Customer Proprietary Network Information Certification
                EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. 64.2009(e) please find attached the 2008 Annual CPNI Certification and Accompanying Statement filed on behalf of Conexiz Corporation.

Please contact the undersigned should you have any questions or concerns at (269) 381-8893 or patrick@crockerlawfirm.com.

Very truly yours,

CROCKER & CROCKER, P.C.

Patrick D. Crocker

PDC/tld

cc: FCC Enforcement Bureau (2 copies via USPS Mail)
         Best Copy and Print, Inc. (via e-mail FCC@BCPIWEB.COM)

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of Company Covered by this Certification: CONEXIZ CORPORATION

Form 499 Filer ID: 826543

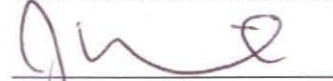Name of Signatory: James M. Wilson

Title of Signatory: President

I am the President of CONEXIZ CORPORATION and as such do hereby certify, affirm, depose, and say that I have authority to make this Customer Proprietary Network Information ("CPNI") Annual Certification of Compliance on behalf of CONEXIZ CORPORATION. I have personal knowledge that CONEXIZ CORPORATION has established adequate operating procedures to ensure compliance with the Commission's CPNI rules as set forth in 47 C.F.R. § 64.2001 et. seq.

Attached to this Certification is an Accompanying Statement explaining how the company's procedures ensure compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

CONEXIZ CORPORATION received no customer complaints in the past year concerning the unauthorized release of CPNI. Further, CONEXIZ CORPORATION has taken no action against data brokers for the unauthorized release of CPNI during calendar year 2008. CONEXIZ CORPORATION will report any information it may obtain with respect to the processes pretexters are using to attempt to access CPNI and what steps CONEXIZ CORPORATION is taking to protect CPNI.

This Certification is dated this ____10____ day of February, 2009.

James M. Wilson
President
CONEXIZ CORPORATION

Customer Proprietary Network Information Certification
Accompanying Statement

CONEXIZ CORPORATION ("CONEXIZ") has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 — 64.2011 of the Commission's rules. This attachment summarizes CONEXIZ's practices and procedures, which have been updated to adequately ensure compliance with the Commission's CPNI rules, as modified by the Commission in 2007.

Safeguarding against pretexting

- CONEXIZ takes reasonable measures to protect CPNI and believes that these measures sufficiently prevent unauthorized access to CPNI.

Training and discipline

- CONEXIZ has trained its personnel in the appropriate use of CPNI. All employees with access to CPNI are required to review CONEXIZ's CPNI policies and procedures.

- CONEXIZ has disciplinary process in place for violations of CONEXIZ's CPNI policies and procedures which would encompass any misuse of CPNI.

CONEXIZ'S use of CPNI

- CONEXIZ does not share, disclose, or otherwise provide CPNI to third parties.

- CONEXIZ may use CPNI for the following purposes:

  > To initiate, render, maintain, repair, bill and collect for services;
  > To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
  > To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent; and
  > To market additional services to customers that are within the same categories of service to which the customer already subscribes.

- CONEXIZ does not disclose or permit access to CPNI to track customers that call competing service providers.

- CONEXIZ discloses and permits access to CPNI where required by law (e.g., under a lawfully issued subpoena).

Customer approval and informed consent

- CONEXIZ does not use CPNI for any purpose that would require customer approval to do so. CONEXIZ does not use CPNI for any marketing purposes and does not share, disclose, or otherwise provide CPNI to any third party. If this policy changes in the future, CONEXIZ will implement practices and procedures to ensure compliance with the Commission's CPNI regulations.

Additional safeguards

- CONEXIZ has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules.

- CONEXIZ designates one or more officers, as an agent or agents of the company, to sign and file a CPNI Compliance Certificate on an annual basis. The Certificate conforms to the requirements set forth in FCC rule 64.2009(e).

- CONEXIZ properly authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-person visit.

- CONEXIZ notifies customers immediately of any account changes.

- CONEXIZ may negotiate alternative authentication procedures for services that CONEXIZ provides to business customers that have both a dedicated account representative and a contract that specifically addresses CONEXIZ's protection of CPNI.

- In the event of a breach of CPNI, CONEXIZ will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs CONEXIZ to delay notification, or CONEXIZ and the investigatory party agree to an earlier notification. CONEXIZ will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.